

CLAIMS

What is claimed is:

1. A method for assigning certificates/private keys to a token, comprising:
 accessing the token through a token reader connected to a computer system by a certificate/private key authority;
 reading a token ID and a user signature certificate from the token;
 searching for a match for the token ID and the signature certificate in an authoritative database;
 creating a certificate, wherein the certificate is wrapped with a public key associated with the token ID and digitally signing the certificate/private key using a signature certificate of the certificate authority;
 downloading the certificate/private key to the token; and
 decrypting the certificate/private key using a private key stored in the token.

2. The method recited in claim 1, wherein the certificate/private key is a plurality of certificates/private keys that at least one certificate/private key is a signature certificate for the user, encryption certificate/private key for the user, and role certificate/private key for the user.

3. The method recited in claim 2, wherein the wrapping of the certificate with the public key of the token encrypts the certificate.

4. The method recited in claim 3, wherein the token is a smart card.

5. The method recited in claim 4, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

6. The method recited in claim 5, wherein downloading the certificate/private key to the token is done through an unsecured communications line.

7. The method recited in claim 6, wherein decrypting the certificate/private key using a private key stored in the token requires the entry of a passphrase by a user.

8. The method recited in claim 11, further comprising:
authenticating, by the signing of the certificate/private key using a signature certificate of the certificate authority, that the certificate/private key was issued by the certificate authority.

9. A computer program embodied on a computer readable medium and executable by a computer for assigning certificates/private keys to a token, comprising:

accessing the token through a token reader connected to a computer system by a certificate authority;

reading a token ID and a user signature certificate from the token;

searching for a match for the token ID and the signature certificate in an authoritative database;

creating a certificate, wherein the certificate is wrapped with a public key associated with the token ID and digitally signing the certificate/private key using a signature certificate of the certificate authority;

downloading the certificate/private key to the token; and

decrypting the certificate/private key using a private key stored in the token.

10. The computer program recited in claim 9, wherein the certificate/private key is a plurality of certificates/private keys that at least one certificate/private key is a signature certificate for the user, encryption certificate/private key for the user, and role certificate/private key for the user.

11. The computer program recited in claim 10, wherein the wrapping of the certificate with the public key of the token encrypts the certificate/private key.

12. The computer program recited in claim 11, wherein the token is a smart card.

13. The computer program recited in claim 12, wherein the token ID is assigned by a token manufacturer at the time the token is created and stored in the authoritative database when assigned to a user.

14. The computer program recited in claim 13, wherein downloading the certificate/private key to the token is done through an unsecured communications line.

15. The computer program recited in claim 14, wherein the decrypting the certificate/private key using a private key stored in the token requires the entry of a passphrase by a user.

16. The computer program recited in claim 15, further comprising:
authenticating by the signing the certificate/private key using a signature certificate of the certificate authority that the certificate/private key was issued by the certificate authority.

FOR OFFICIAL USE ONLY